i o t t
Intelligence To Action

CYCURA™
Our tools, your security

FORENSIC REPORT

Andrea Tantaros

Mobile Forensics - Blackberry

DATE: JANUARY 23, 2018
PREPARED BY: CYCURA
FOR: AIG
DELIVERED TO: JOSEPH CANE, ESQ.

PROJECT CODE: CYCF-AIG-FI-A03

Intelligence To Action

Andrea Tantaros – Mobile Forensic Report

Executive Summary

Cycura Inc was engaged by Andrea Tantaros to forensically review a Blackberry Mobile Phone she was using during the time period of 2016. The goal of the examination was to determine if any applications had been loaded such as key loggers or other monitoring applications.

After an initial review of the Blackberry, Cycura determined the operation system version to be 10.3.2.556. This particular operating system from Blackberry has very limited support from the mobile forensic application vendors and as such our ability to preserve and extract information was also quite limited. The Blackberry operating system does not allow us to go to the depth of being able to physically capture raw data or application data.

Cycura utilizes world class leading forensic applications and has developed in house methodologies for preserving and capturing data. Once Cycura had preserved all the available data at a logical file system level, we then attempted to backup the Blackberry using Blackberry Link. We were successful in connecting to the Blackberry, however, the permissions on the Blackberry at an administration level did not allow us to perform a backup of the device. We were able to view the information using Blackberry Blend, however this was the same information we had captured during the logical preservation. Cycura was able to preserve (321) contacts, (164) text sms messages, (23) mms messages and (13) email messages.

After reviewing the available data Cycura determined the “corporate” workspace was most likely deleted from the Blackberry Enterprise Server administrator. The Blackberry contains very limited data and applications which would lead us to believe there was another workspace. During our review of the mobile phone, we observed there was no Blackberry ID set, no PIN messages, no device password, no corporate applications and no encryption setting. All of these settings and features would normally be turned on. Cycura understands corporate Blackberry’s such as these are normally connected to a Blackberry Enterprise Server “BES” at a remote location. The BES has the ability to set policy, perform backups, delete data, push applications and services and basically remotely control the phone.

Intelligence To Action

Given our conclusion that this Blackberry was most likely connected to and controlled by a BES, the only available backups would be on the BES. This would also allow any administrator in control of the BES to be able to pull the backup of the device and view all the data. This would also include all the data that is not available to mobile forensic applications such as application data, history files, and log files.

Appendix

Phone Examination Preview Report – Blackberry 9EE6

Selected Manufacturer:	BlackBerry CDMA
Selected Model:	SQC100-3 Classic
Detected Model:	Classic
ESN:	990004601441318
ICCID:	89148000002105181553
Connection Type:	USB Cable

Phone Examination Report Index

Contacts (321)	Selected
S - Text Messages (164)	Selected
Error! Hyperlink reference not valid.	Not Supported

Intelligence To Action

Error! Hyperlink reference not valid.	Not Supported
; - Multimedia Messages (23)	Selected
Email Messages (13)	Selected
Error! Hyperlink reference not valid.	Not Supported
Error! Hyperlink reference not valid.	Not Supported
Browser History	Not Supported
Web Searches	Not Supported
Error! Hyperlink reference not valid.	Not Supported
Error! Hyperlink reference not valid.	Not Supported
Error! Hyperlink reference not valid.	Not Supported
Error! Hyperlink reference not valid.	Not Supported
Error! Hyperlink reference not valid.	Not Supported
Error! Hyperlink reference not valid.	Not Supported

Allowing BlackBerry 10 users to back up device data

You can control whether BlackBerry 10 users can back up and restore device data. You can permit users to back up only data from the personal space or to back up data from both the personal and work spaces. In the IT policy that you assign to users, you can select one or both of the following IT policy rules:

IT policy rule	Applicable activation types
Allow backup and restore of device	❒ Work and personal - Regulated ❒ Work space only
Allow backup and restore of work space	❒ Work and personal - Corporate ❒ Work and personal - Regulated ***Note:*** *For devices activated with "Work and personal - Regulated," this rule is applied only if the "Allow backup and restore of device" rule is selected.*

If the IT policy that is assigned to users permits device backups, users can log in to BlackBerry Link to create or restore back up files.

When users create backup files using BlackBerry Link, the files are encrypted using encryption keys that BlackBerry UEM sends to BlackBerry 10 devices. The initial encryption keys are generated when you install or upgrade to BlackBerry UEM version 12.4. If necessary, you can generate new encryption keys, import encryption keys from another BlackBerry UEM instance, or export encryption keys.

https://help.blackberry.com/en/blackberry-uem/12.6/administration/amo1449171259072.html

Using IT policies to manage devices

An IT policy is a set of rules that restrict or allow features and functionality on devices. IT policy rules can manage the security and behavior of devices. The device OS determines the list of features that can be controlled using IT

policies and the device activation type determines which rules in an IT policy apply to a specific device.

Only one IT policy can be assigned to each user account, and the assigned IT policy is sent to all of the user's devices. If you don't assign an IT policy to a user account or to a group that a user or device belongs to, BES12 sends the Default IT policy to the user's devices.

You can rank IT policies to specify which policy is sent to devices if a user or a device is a member of two or more groups that have different IT policies and no IT policy is assigned directly to the user account. BES12 sends the highest ranked IT policy to the user's devices.

BES12 automatically sends IT policies to devices when a user activates a device, when an assigned IT policy is updated, and when a different IT policy is assigned to a user or group. When a device receives a new or updated IT policy, the device applies the configuration changes in near real-time.

Devices ignore rules in an IT policy that to not apply to them. For example, BlackBerry 10 work space only devices ignore rules that only apply to BlackBerry Balance devices or to a different device OS

https://help.blackberry.com/en/bes12/12.4/security/kja1394733650229.html

Remove Secure Work Space from devices

You can remove Secure Work Space from devices. For example, if you want devices to use BlackBerry Work instead of Secure Work Space, you can assign a Good Dynamics profile to a user and then remove Secure Work Space from the devices. When you remove Secure Work Space from devices, users are not required to reactivate their devices.

1. On the menu bar, click **Users**.
2. Select the users that you want to remove Secure Work Space from.

3. Click  .

4. When you are prompted to remove Secure Work Space from the selected users' devices, click **Remove**.

When you remove Secure Work Space from a device the activation type that is assigned to the device changes as follows:

- Devices that are activated with Work and personal - full control are assigned the MDM controlsactivation type
- Devices that are activated with Work and personal - user privacy are assigned the User privacyactivation type

https://help.blackberry.com/en/blackberry-uem/12.6/administration/esk1449